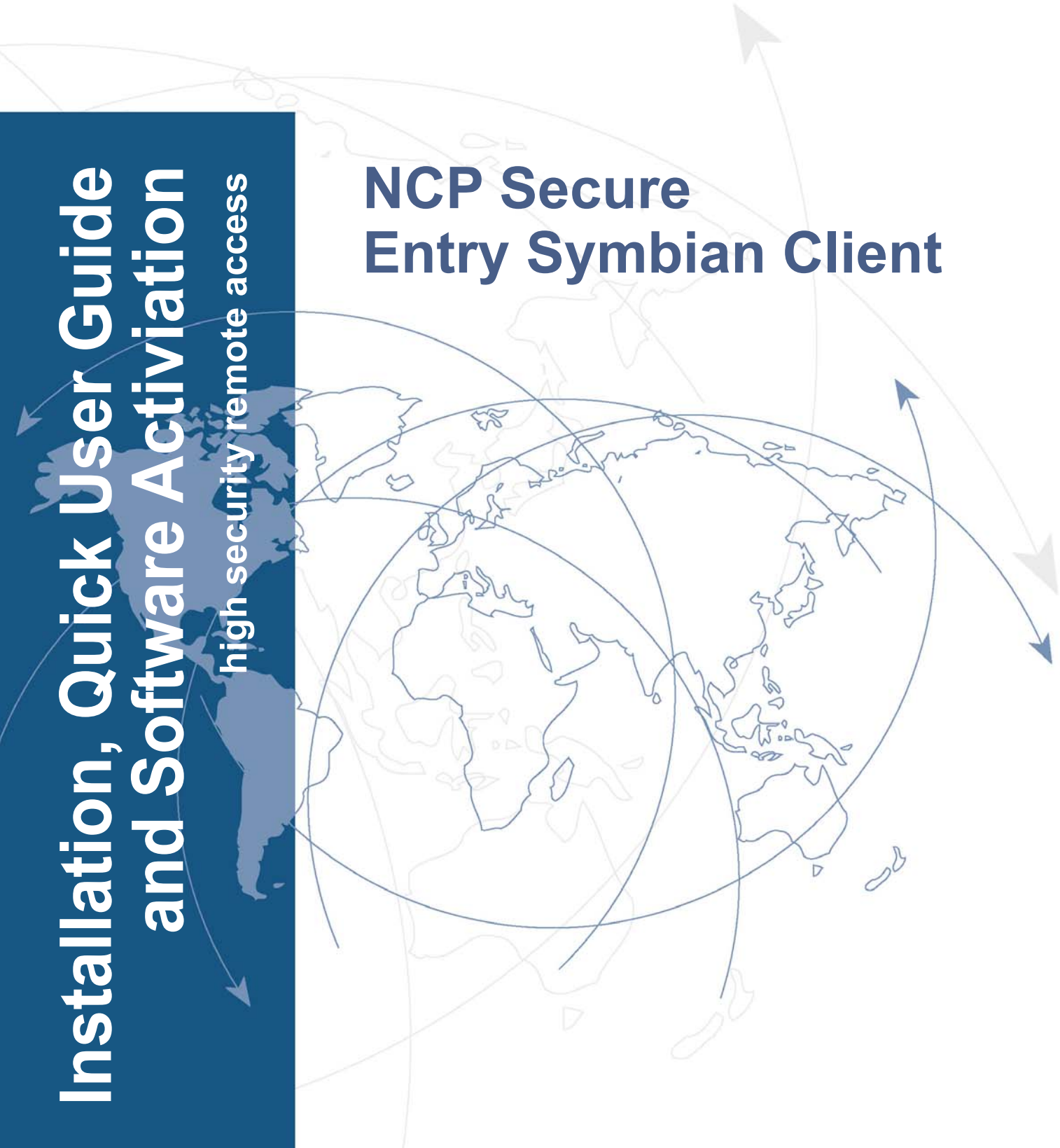
NCP
SECURE COMMUNICATIONS

NCP Secure Entry Symbian Client

Installation, Quick User Guide and Software Activation

high security remote access



Entry Symbian Client

Installation Description, Quick User Guide and Software Activation

Network
Communications
Products engineering GmbH

GERMANY
Headquarters:
Dombühler Straße 2
D-90449 Nürnberg
Tel.:+49-911-99680
Fax: +49 - 911 - 9968 299
Internet
http://www.ncp-e.com/en
E-mail: info@ncp-e.com

Copyright

Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.
NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly-disclaims all expressedor impliedwarranties of merchantability or usefor anyparticular purpose.
Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.
This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© NCP engineering GmbH, July 2008
All rights reserved.

NCP Hotline

NCP offers support for all international users by means of Fax and Internet Mail.

Fax Hotline Number: +49 911 99 68 458

Internet Mail Address: support@ncp-e.com

When contacting NCP with your problems or queries
please include the following information:
– exact product name
– serial number
– version number
– accurate description of your problem
– any error message(s)
Homepage von NCP: http://www.ncp-e.com

Contents

Installation Description, Quick User Guide and Software Activation

1. Installation Prerequisites 6
1.1 Installation of the PC Component 8
Installing from Hard Disc 8
Installing from NCP CD 8
1.2 Installing the NCP Client Phone Component 10
Starting the Secure Client 11
Uninstalling the NCP Secure Entry Symbian Client 11
1.3 Configuring Destination Systems 12
Configuration Assistant 12
– Profile Name 12
– Connection Medium (Dial-up Configuration) 12
– Access Point 12
– VPN Gateway Parameters and Extended Authentication 12
– IPSec Configuration 13
– Pre-shared Key 13
– IPSec Configuration, IP Addresses 13
– Link firewall 13
Profile Settings 14
Uploading and Downloading the Profile Settings 15
Profile Settings Backup 15
Uploading 15
Downloading 15

2. Quick User Guide 16
Main Monitor 16
Select another Profile 17
Establishing a Connection 17
Username and Password 17
Selecting an Access Point 17
Closing the Monitor 18
Terminating the VPN Tunnel 18
Statistics and Log Entries 18

3. Licensing via Activation Dialog 19
Test Version Validity Period 19
Software Activation 20
Online-Variante 20
Offline Variant 21
Step 1 21
Step 2 22

Installation, Quick User Guide and Software Activation

This document describes the installation of the NCP Secure Entry Symbian Client (consisting of PC and phone components), the transfer of configuration data between these components and the activation of the software.

PC component:

NCP Entry
Configuration Manager Symbian

This component is used to create phonebook entries (VPN profiles) and to synchronise the data file on the phone.

Phone component:

NCP Secure Entry Client

NCP Secure Enterprise Client is installed on the mobile end device (phone) and is used to establish a connection to a VPN gateway. A destination system for the VPN connection can be selected from the integrated phonebook. The client monitor also shows the status of the connection to the VPN gateway.

For more information on extensions and product versions, please go to the NCP website at http://www.ncp-e.com

1. Installation Prerequisites

The software is easily installed using Setup. The procedure is the same for all versions of this software.

The following system requirements must be met to install and use the software:

PC component:
NCP Entry Configuration Manager Symbian

The current version of the Nokia PC Suite and one of the permitted operating systems must have been installed first. The mobile device with the Nokia PC Suite must be linked to the PC before the phone components are installed.

Operating systems: Windows 2000, Windows XP, Windows Vista;
approx. 32 MB RAM and 15 MB free hard disc space.

Phone Component:
NCP Secure Entry Client

The mobile device will need to be booted by switching it off and on after installation of the NCP Secure Client.

Operating systems: only Symbian OS v 9.1 or later as the basic system;only Nokia Series S60 3rd Edition and later* as the interface;
approx. 3 MB RAM and approx. 2 MB free data space

** For more information on extensions and product versions, please go to the NCP website at http://www.ncp-e.com*

© NCP engineering GmbH / 1.00

The following condition must be met for data transfer between the components:

Nokia PC Suite

The current version of Nokia PC Suite must be installed on the PC. This software is supplied with your Nokia mobile phone. If you accept the recommended standard installation of Nokia PC Suite, the software will install automatically using Autostart. The connection between the PC and phone via the USB cable (or Bluetooth) will also be automatic.

Software Language

Please note that English or German can be selected as the language for the user guide, including the NCP Secure Symbian Client online help. Additional native languages are not supported at this time.

After installation, the PC components are presented in the language selected at the beginning of the installation as installation language, independently from the system language that is active on the PC. The language can be reset subsequently on the Configuration Manager window menu.

After the installation, the phone components that are active at the time point of installation as phone language are presented automatically: If the smart phone's user interface is English, the client user interface also appears in English; if it is German, it appears in German. If the phone language is neither English nor German, you are given the opportunity to select between German and English in a dialog box during installation of phone components.

The language of the phone components assigned upon installation can no longer be subsequently changed, even should the mobile device phone language be reset. The single possibility to change the language for the phone components is a new installation.

Sequence from Installation to Starting

Please follow the order below.

– Installation of current version of Nokia PC Suite

– Installation of "Configuration Manager"
PC component

– Installation of "NCP Secure Client"
phone component on the mobile device

– Restart mobile device by switching off and on

– Creation of phonebook with
Configuration Manager

– Transfer of phonebook to mobile device

– Start using phone

1.1 Installation of the PC Component Configuration Manager

After the current version of Nokia PC Suite has been installed, the Configuration Manager for the NCP Secure Entry Symbian Client can be installed.

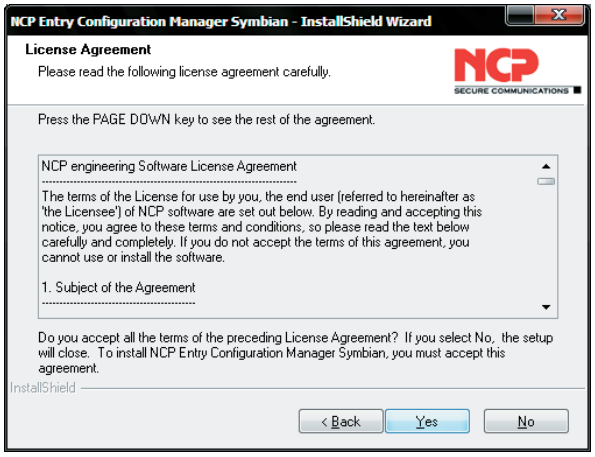
The Configuration Manager later configures the destination system (VPN profile), the composition of the phonebook, and its transfer to the phone (see “Destination System” section below).

Installing from Hard Disc

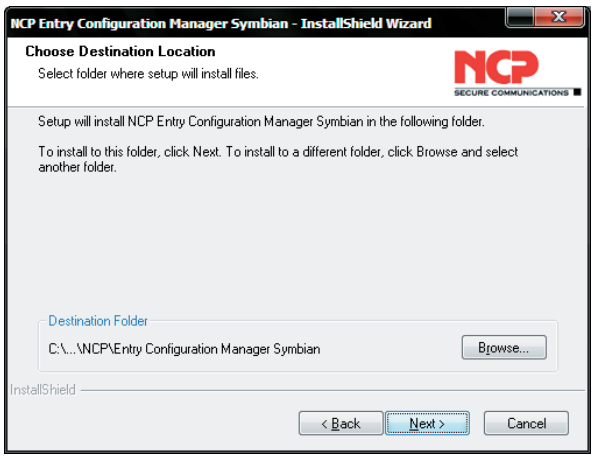
If you prefer to install the software by downloading it from the NCP website, unzip the ZIP file in one of your directories. A “DISK1" subdirectory will be created automatically. In ”DISK1", start the installation program:
NCP_EntryCl_Symbian_xxx_yyy.EXE*
The rest of the installation is the same as from the NCP CD.
* x = version number, y = build number

Installing from NCP CD

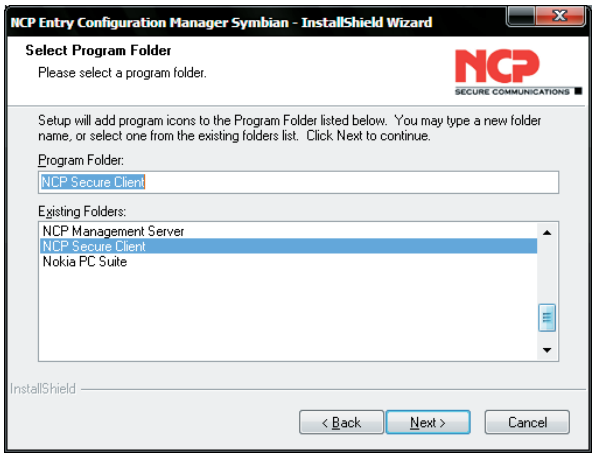
Insert the CD in the drive and wait a couple of seconds for the NCP welcome page to appear on your monitor. Select the product to be installed and click on “Install product”.


NCP Entry Configuration Manager Symbian - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
NCP
SECURE COMMUNICATIONS
Press the PAGE DOWN key to see the rest of the agreement.
NCP engineering Software License Agreement
The terms of the License for use by you, the end user (referred to hereinafter as 'the Licensee') of NCP software are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read the text below carefully and completely. If you do not accept the terms of this agreement, you cannot use or install the software.
1. Subject of the Agreement
Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install NCP Entry Configuration Manager Symbian, you must accept this agreement.
InstallShield
< Back
Yes
No

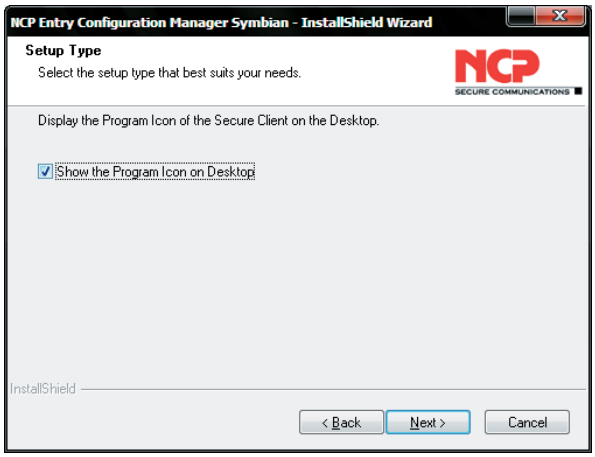
The NCP Secure Symbian Client is installed on your computer as soon as the Setup programme has prepared the Install Shield Assistant. First read the license conditions carefully, then click on “Yes”.


NCP Entry Configuration Manager Symbian - InstallShield Wizard
Choose Destination Location
Select folder where setup will install files.
NCP
SECURE COMMUNICATIONS
Setup will install NCP Entry Configuration Manager Symbian in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\NCP\Entry Configuration Manager Symbian
Browse...
InstallShield
< Back
Next >
Cancel

Then choose the destination directory for the client software (normally Programme\NCP\Entry Symbian Configuration Manager), and click on “Next”.


NCP Entry Configuration Manager Symbian - InstallShield Wizard
Select Program Folder
Please select a program folder.
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.
Program Folder:
NCP Secure Client
Existing Folders:
NCP Management Server
NCP Secure Client
Nokia PC Suite
InstallShield
< Back
Next >
Cancel

Specify the programme file (normally “NCP Secure Client”) and click on “Next”.


NCP Entry Configuration Manager Symbian - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Display the Program Icon of the Secure Client on the Desktop.
Show the Program Icon on Desktop
InstallShield
< Back
Next >
Cancel

In this window, you can place a programme icon for starting the Configuration Manager on the desktop. Click on “Next”.

The Setup programme carries out the desired operations and installs the Configuration Manager on the hard disc.

Click on “Finish” to end installation. The computer does not need to be rebooted.

Leaving the setting “Start mobile device installation”, the installation of the phone component will be started after finishing automatically.

Removing this setting, the phone component can also be installed later. See the chapter “ Installating NCP Client Phone Component”.

1.2 Installing the NCP Client Phone Component

The phone component can be installed as soon as there is a connection to the mobile device via Nokia PC Suite. To connect:

PC end

After the “NCP Secure Client” programme group has been installed, you will find the “Entry Symbian Configuration Manager” programme in the Windows start menu.

Start the Configuration Manager from the programme menu (or desktop icon).

If a confirmation window appears, you can click on “Yes” to create a destination system using an assistant (see “Destination system” below). However, this is not necessary for the installation.

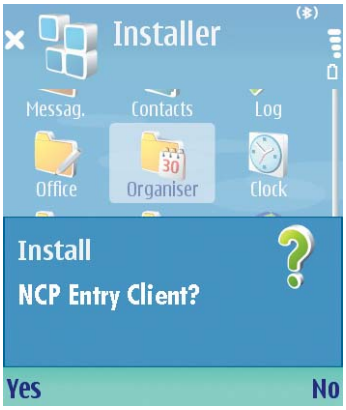
Confirmation
There is no destination for the VPN dial-up!
Do you want to use the Configuration Assistant for generating a destination entry now?
Yes
No

Click on “No” to continue installing the phone component.

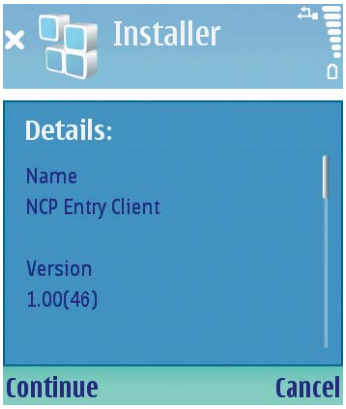
Select “Install system / mobile device” in the Configuration Manager menu (see illustration below).

Phone end

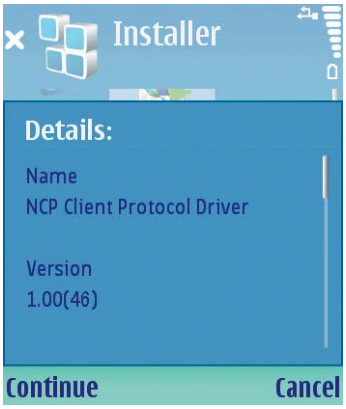
You install the phone components using the display on your mobile device. You will first require Nokia PC Suite to install the NCP Secure Entry Symbian Client on your mobile device.



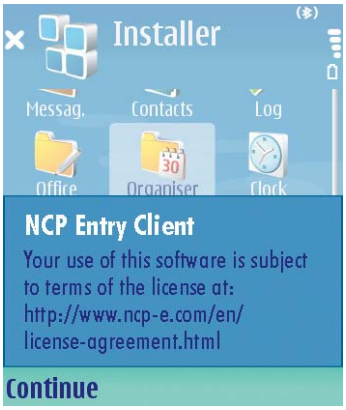
A question will appear on the phone’s display, asking whether you want to install the client. Press “Yes”.



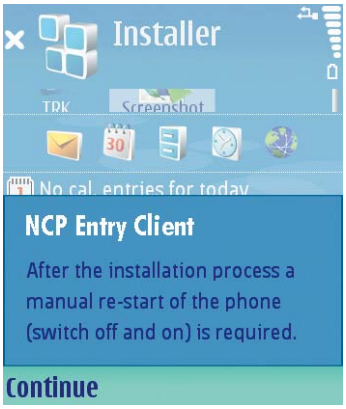
The product details and version will appear. Press “Continue”.



The following window informs about installing the protocol driver. Press “Continue”.



Press “Continue”.


Installer
No cal. entries for today
NCP Entry Client
After the installation process a manual re-start of the phone (switch off and on) is required.
Continue

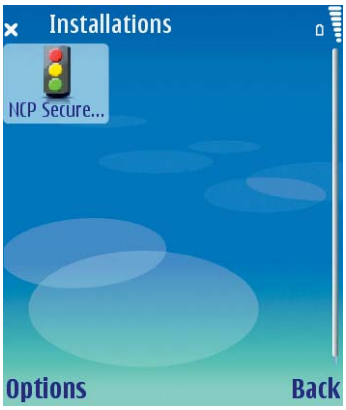
You will be told you have to boot your mobile device after installation. Press “Continue”. (See illustration left)

Press “Continue”.

The installation process will be displayed.

When it finishes, reboot your mobile device by switching it off and on..

The NCP Secure Client is inserted in the installation directory.



You press on the icon to start it.

Starting the Secure Client

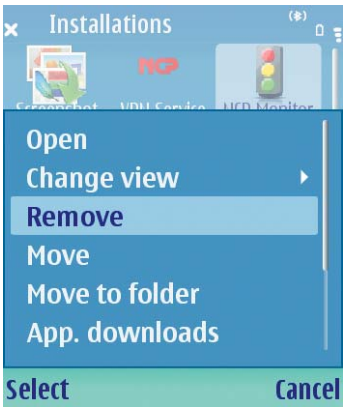
After installation of the NCP Secure Client on the Smartphone under “Installed programmes”, you need to restart the mobile device by switching it off and on.

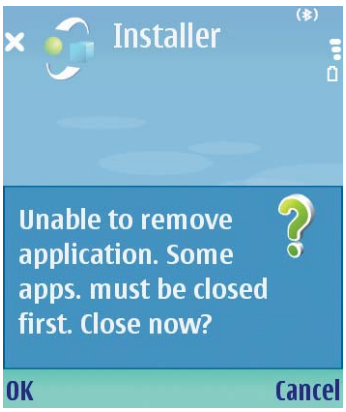
Each time the phone is switched on, the VPN service from NCP is automatically loaded in the background, so a VPN connection to the configured destination system can be made immediately after the NCP Secure Client starts (see “Configuring Destination System” below).

Uninstalling the NCP Secure Entry Symbian Client

The PC component of the Client is uninstalled using Windows System management / Software / Components.

The phone components are uninstalled using the system manager on the mobile device. The driver for the NCP Secure Client is deleted at the same time. The mobile must be switched off and on again to delete the driver from memory.



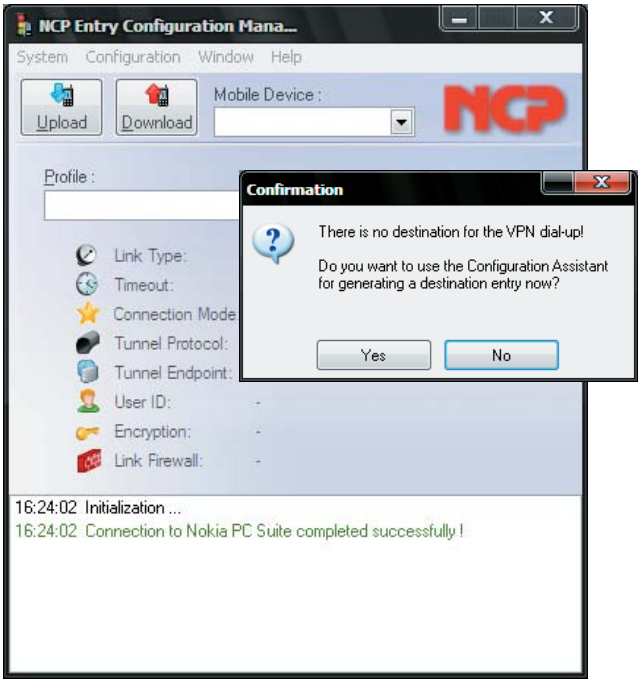


The VPN service running in the background must be terminated (closed). To do so, click on “OK”.

1.3 Configuring Destination Systems

A destination system is a profile setting in the Configuration Manager, where the most important parameters are defined: where and how a VPN connection from the NCP Secure Client is established on the mobile phone. A connection between the smartphone and the destination system can not be established (see “Establishing a connection”) without configuring a destination system and transferring it to the mobile device (see “Phonebook / Uploading”).

After the PC component has been installed using the Configuration Manager (see above), start the Configuration Manager from the Programme menu (or desktop icon). The confirmation window appears at the same time as the Configuration Manager interface. Press “Yes” in this window to start a configuration assistant automatically. The assistant is used to configure the first destination system or to create the first profile setting.



Configuration Assistant

The configuration assistant also starts when you want to add a new entry to the profile settings under “Configuration / Profile Settings” in the menu (see “Profile Settings” below).

IPSec connections to the company network can be established quickly using the configuration assistant. It brings up the most vital parameters. Once you have accepted the entries in these fields, a new profile is created. Standard values are entered for all other parameter fields in the profile settings; you can change these at a later time (see “Configuration Manager parameters” below). The profile will be stored in the profile settings after a few configuration queries, depending on the basic setting chosen.

The sections below describe the parameters for configuring a connection to the company network via IPSec. The square brackets contain the parameter fields found in the Configuration Manager (also refer to the online help for the Configuration Manager and the description “Mobile Client Parameters”):

– Profile Name

Enter a distinctive name for the destination system. It may include both alphanumeric and numeric characters, and be 39 characters long, including spaces [Basic Settings].

– Connection Medium (Dial-up Configuration)

You select the connection type to be established via the tunnel. The type can be specific to each destination system, provided you have the appropriate hardware connected and installed on your system (only “Symbian Internet access point” can be used with the current Symbian operating system [Basic Settings].

– Access Point

Different access points can be stored in the Smartphone (e.g. T-Mobile Internet or WLAN access point). These configured access points appear when setting up the connection for “Selection on mobile device” (see “Connection set-up” below) [Basic Settings].

– VPN Gateway Parameters and Extended Authentication

For which VPN gateway, i.e. which tunnel end point, should the IPSec connection be set up? Indicate here the official IP address or the DNS name

via which you can reach the VPN gateway. In the case of an IPSec connection, you can also use extended authentication additionally to the authentication via a pre-shared key [IPSec General Settings, Identities].

Enter your code words, VPN user name and VPN password, for the tunnel connection here. (They also will be used for extended authentication, when activated; see above). If you do not want to save the password, it will be requested each time a connection is established [Identities].

– IPSec Configuration

The IPSec negotiation will use “automatic mode” which are pre-defined (default) proposals. In the event that uniquely defined IKE- and IPSec policies are to be used, these can then be defined and assigned using the policy editor [IPSec General Settings].

– Pre-shared Key

Common keys can be used for data encryption. Enter the key here (static key, pre-shared key) that must be stored on both sides - client and gateway. The associated string must be entered for the IKE ID, depending on selected IKE ID type [Security].

– IPSec Configuration, IP Addresses

Specify which IP address the client is going to use. By selecting “Use IKE Config Mode” the clients IP address is dynamically assigned by the VPN gateway. IF DNS / WINS server are used, you can define their IP addresses [IP Address Assignment].

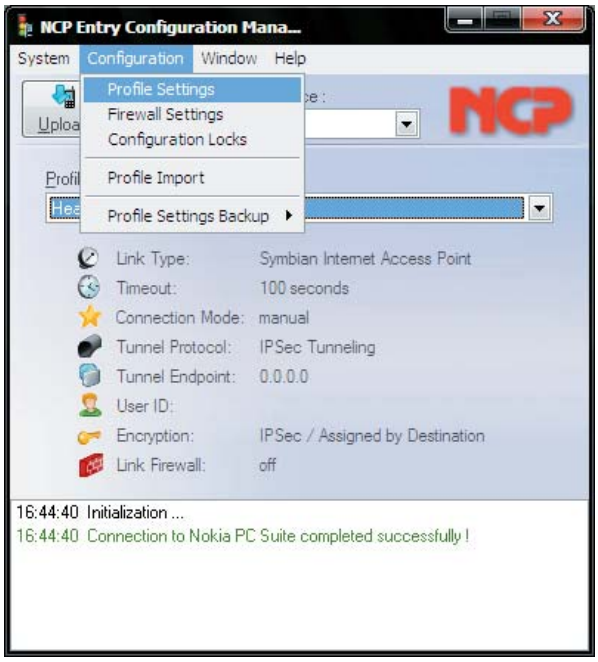
– Link firewall

The settings for Link firewall apply only to the destination system configured here (the global firewall settings, on the other hand, are valid for all links). If you activate Stateful inspection, no data packets will be accepted from other hosts [Link firewall].

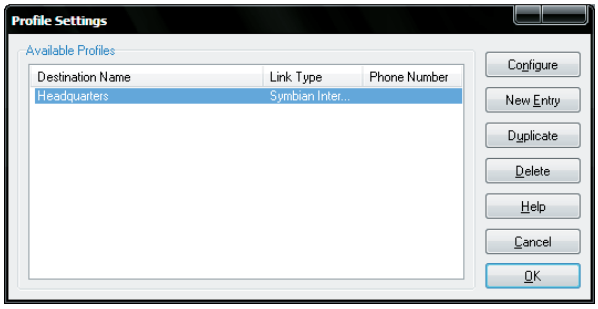
Once you click on “Finish”, the first profile setting of the first destination system is stored (see illustration below.

Profile Settings

The profile settings are entries for alternate destination systems, i.e. different configuration profiles for establishing a connection to a VPN gateway. These configuration profiles can be regenerated or modified by selecting “Configuration / Profile Settings” in the Configuration Manager menu.

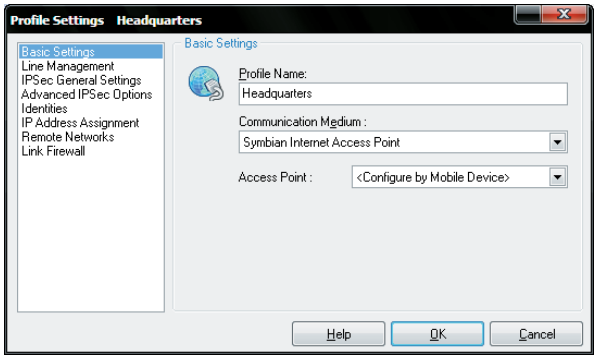


The profile settings display a list of already available destination systems, with name, connection type (and call-up number, if applicable). Double-clicking on a destination system allows the configuration to be viewed and/or changed. The buttons on the right-hand side should be used as required. Pressing “Cancel” stores the entries without changes. Selecting “OK” accepts the changes before closing the profile setting.



If you want to modify the entry you have created with the assistant, click on “Configure” and select the parameter field where the assistant has put your entries (see “Configuration Assistant” above).

The illustration below shows the “Destinationsystem” parameterfield for the pho-nebook entry “Headquarters”.



You can find a detailed description of creating destination systems and the meaning of the parameters in the description of the “Mobile Client Parameters” or in the Configuration Manager online help.

Because configuration profiles cannot be created on the smartphone, they must first be created in the Configuration Manager and then transferred to the smartphone.

Uploading and Downloading the Profile Settings

Profile Settings Backup

Please note that an existing profile setting on the mobile device will be always overwritten without asking if a new profile setting is uploaded. Similarly, a profile setting on the PC will always be overwritten when a profile setting is downloaded from the phone. If different profile settings for different mobile devices, for example, are to be stored, this can only be done on the PC by renaming the file ncpphone.cfg in the user directory.
(Documents and Settings\User\Application Data\NCP\Entry Configuration Manager Symbian\bin\ncpphone.cfg)

Profile settings backup via the Configuration Manager is only intended for recovering the last profile setting; the backup file ncpphone.sav is renamed again as ncpphone.cfg.

Uploading

The profile settings-file with the configured destination systems is transferred to the Smartphone as follows:

Switch on the smartphone and establish a connection between the PC and the smartphone using PC Suite. Then press the “Upload” button in the Configuration Manager.

The transfer to the smartphone fails and a corresponding error message appears on the PC, if the mobile device is not rebooted after installation of the client (i.e. if the VPN service is not running). In this case, start the smartphone again by switching it off and on, then press the “Upload” button in the Configuration Manager once more.

If the NCP Secure Client has already started with an older profile setting, the older profile setting will be overwritten and the NCP Secure Client will automatically load the new once.

If at the time of the upload there is a VPN connection from the NCP Secure Client to one of its destination systems, the existing connection will be cut by the upload without warning and the older profile setting overwritten.

Downloading

Press the “Download” button in the Configuration Manager to download a profile setting from the mobile device to the PC. (In this case too, the mobile device must be started and a connection established between the PC and the smartphone using PC Suite.)

During downloading of the profile setting from the smartphone to the PC, the profile setting on the PC will be overwritten. If an existing profile setting on the PC is to be retained, it must have its own backup. It is located as file ncpphone.cfg in the user directory (see above).

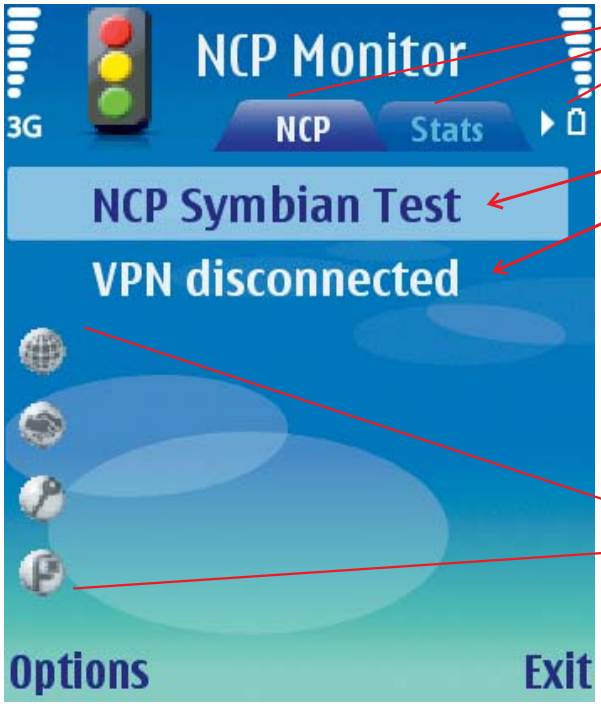
If a download fails, despite there being a connection between the PC and the smartphone, the mobile device needs to be rebooted by switching it off and on again.

2. Quick User Guide

Once you have transferred the profile settings with the configured destination systems to the smartphone, you can select a profile which was configured on the Entry Configuration Manager Symbian.

Main Monitor

When you have started the client, the main monitor displayes the destination system highlighted which was selected in the configuration manager. (Illustration below).



Tabs:

There are three tabs: NCP, Stats and Log.
The NCP tab displays:
the **current profile** and
the **VPN tunnel state**.

Stats:

Statistics and informations of the current connections

Log:

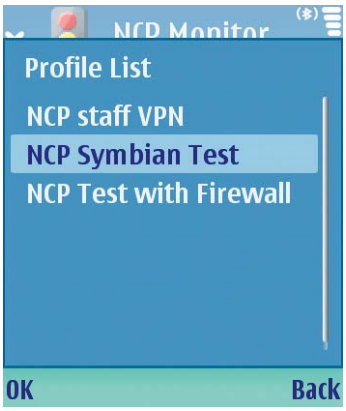
(In the picture of the left not displayed)
Log entries for support purposes

Status displays:

The client monitor displays different icons depending on the configuration; these icons can change the colors from grey to green depending on the phases of the connection setup.

Select another Profile

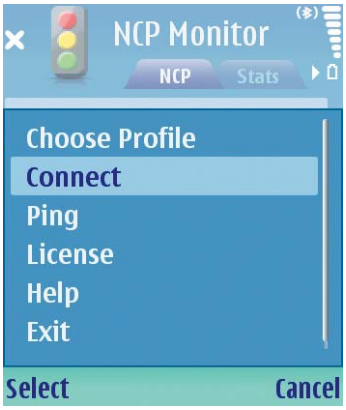
To select another destination system, press the action button or "Options" and afterwards "Choose Profile". (Illustration on the left).



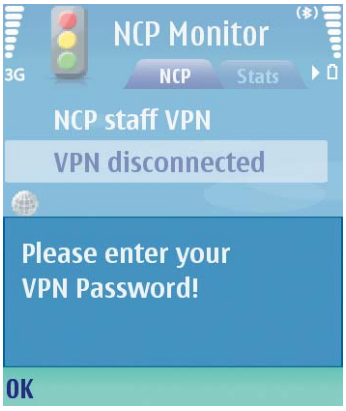
When selected the required destination system from the list, press "OK".

Establishing a Connection

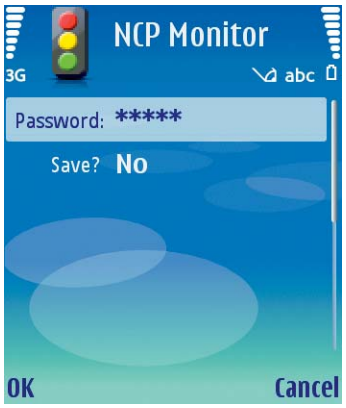
To establish the VPN tunnel to the destination system press the line with the tunnel state or "Options" and then select "Connect". (In this case: VPN disconnected)



Username and Password

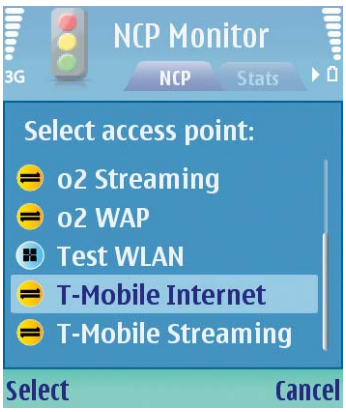


If username and/or password was not entered in the phonebook of the configuration manager it will be required when the connection is going to be established. Press "OK" and enter your password.



When you have entred username and/or password you can save the entry in the phonebook on the smartphone by pressing "save". Then press "OK".

Selecting an Access Point

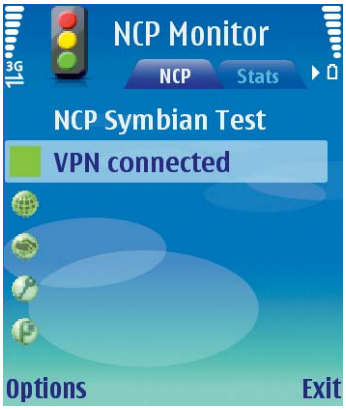


After that select one of the preconfigured internet access points (IAP) and press "Select".

Now the connection will be established.

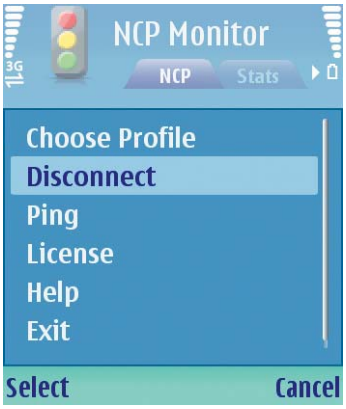
When starting an application (E-Mail, Web Browser) be sure that the IAP is the same as the one for the tunnel connection!

Closing the Monitor



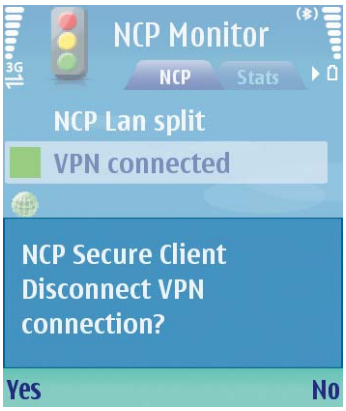
By pressing “Exit” the Monitor can be closed, but the connection will not be disconnected because the client will be active in the background.

Terminating the VPN Tunnel



After finishing the application you can terminate the tunnel connection by pressing the menu “Options / Disconnect” ...

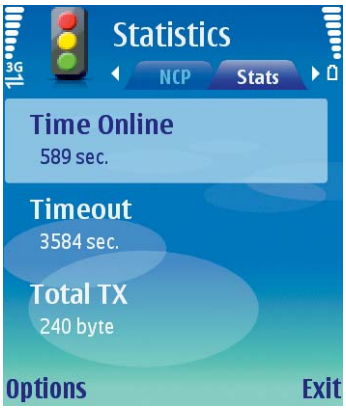
... or by highlighting the tunnel status and then press the action button.



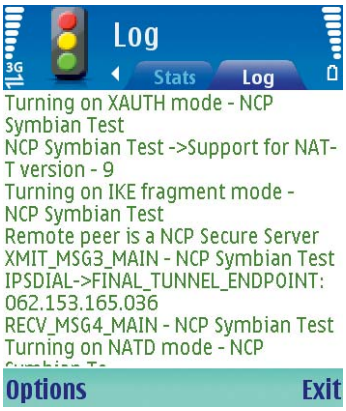
When this question in the monitor (see picture on the left) is displayed, press “Yes” and the tunnel will be terminated.

Statistics and Log Entries

Selecting the tabs “Stats” and “Log” in the main monitor, you can read statistics and log entries of the current VPN tunnel connection.



The statistic data display connection infos about: Time Online, Timeout, Total Tx/Rx Bytes; encryption, Security Mode and views the own VPN IP address.


Log
Stats
Log
Turning on XAUTH mode - NCP Symbian Test
NCP Symbian Test ->Support for NAT-T version - 9
Turning on IKE fragment mode - NCP Symbian Test
Remote peer is a NCP Secure Server
XMIT_MSG3_MAIN - NCP Symbian Test
IPSDIAL->FINAL_TUNNEL_ENDPOINT: 062.153.165.036
RECV_MSG4_MAIN - NCP Symbian Test
Turning on NATD mode - NCP
Options
Exit

The log windows shows informations to enable qualified system technicians to perform low level traces for fault finding and debugging purposes.

© NCP engineering GmbH / 1.00

3. Licensing via Activation Dialog

The client software is always installed as a test version. After a new or pre-installation, the client needs to be activated. An older version which has been upgraded, will be during the upgrade process be reset to a test version and so too requires to be activated within 30 days.

The activation dialog is opend using the popup menu "Activiation" or by pressing on "Yes" when the message box is displayed after the start of the NCP client service. (Illustration on the left)

The time remaining until software activation is required, i.e. the validity period of the test version, is displayed in the license information. (Illustration on the left)

In order to use a full version with no time limitations, the software must be released version shown in the activation dialog with the license key and the serial number that you have received. The activation dialog can be opened using the arrow button in the license information message.

The license data can be entered either online or offline via a wizard.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the NCP aczivation server, and the activation key that is then displayed on the website must be noted. This activation key can be entered in the licensing window of the Monitor menu at a later point in time.

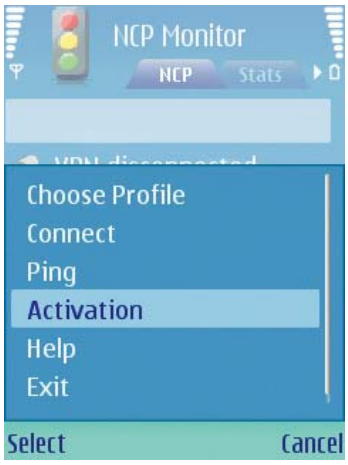
In the online variant, an assistant forwards the licensing data to the activation server immediately after entry and thus allowing the software to immediately be released.

Test Version Validity Period

The test version is valid for 30 days. Without software activation or licensing it will no longer be possible to setup a connection after this 30-day period expires.

After installation, each time the software is started the validity period will be shown in the popup window once a day.

The software can be used during the trial period when clicking "No" in the activation dialog.



When the trial period has expired the software must be either activated or deinstalled. To activate, start the activation dialog by pressing the "OK"-button.

Software Activation

When the test phase has expired (see illustration on the left), the software must be either activated or de-installed. To activate, select the menu option “Activation” in the popup menu.

Here you can see which software version you have and how the software is licensed, i.e. you can see that the test version has expired and that the software has not yet been activated/licensed. To activate click the arrow button right above.

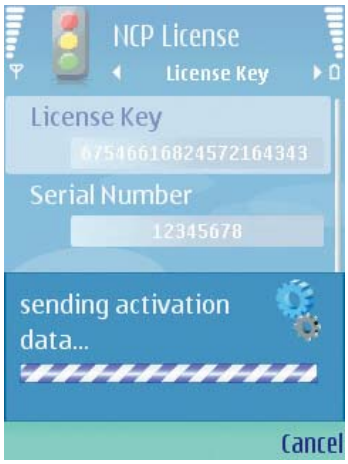
In the window that appears, select whether you wish activate the client online or offline by selecting either online activation or offline activation respectively.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the NCP activation server, and the activation key that is then displayed on the website must be noted. In the online variant, an assistant forwards the licensing data to the web server immediately after entry and thus the software is immediately released.

After selecting the type of activation (see “Online” on the left) the license data is to be entered in the appropriate fields.

Click on the arrow button on the right to continue.

Online-Variant



With the online variant the license data will be transmitted to the NCP Activation Server via an Internet connection. This Internet connection can either be established via an IAP on the telefone.

(If a proxy server has been configured on the IAP it will be used automatically.)

The activation assistent requires a connection to already be established.

Click on the arrow button on the right to continue. The software is activated automatically.

As soon as the activation server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with online activation the new license key will be transferred automatically (license update), and the new features of the software will be available to use.

Write down the update key for the next activation or for reinstallation.

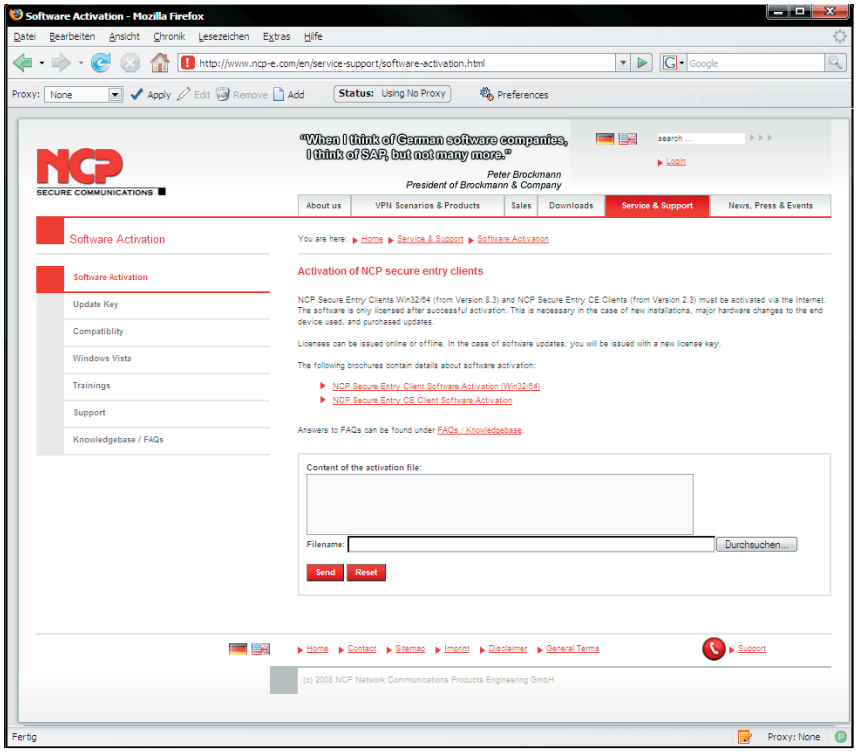
Upon completion of the activation process, the software version number may differ from the licensed version number if the license is valid only for an older version. (Illustration above)

© NCP engineering GmbH / 1.00

Offline Variant

The offline variant is executed in two steps. In the first step a file is generated after entering the license key and serial number, and is then sent to the NCP activation server. The URL is:
`http://www.ncp-e.com/en/service-support/software-activation.html`

An activation key will be shown on the web site, and you must note this number in order to enter the license key in the licensing window of the activation dialog in a second step. (Which can also be executed at a later point in time.)


Software Activation - Mozilla Firefox
"When I think of German software companies, I think of SAP, but not many more."
Peter Brockmann
President of Brockmann & Company
Software Activation
Activation of NCP secure entry clients
Content of the activation file:
Filename:
Send
Reset

Step 1

The offline variant can be initiated via the activation dialog and can be selected in the first window. (Illustration on the left).

With the first step a file for activation will be created. This step will be selected automatically. Click on the arrow button on the right. In the following window enter the license data and click on the arrow button.

Now an activation file is created and this file must be transferred to the activation server. Pathname of the activation file always is:

`C:\Data\NCP\NCPactivation.dat`

Now copy the file to the PC using Nokia PC Suite. After that the NCP web site must be called (illustration above):
`http://www.ncp-e.com/en/service-support/software-activation.html`

There are two ways to transfer the activation file to the Activation Server. Either copy the content of the activation file with Copy & Paste, after you have opened the activation file with the Notepad (ASCII editor), into the window that is open on the web site, or click on the “Browse” button and select the activation file. Click on “Send”! Then the activation code will be generated and displayed on the web site.

Note the activation code and continue the activation process under the menu option “Help” / License data and activation", by executing the second step of the activation in the offline variant.

If the activation server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with the online activation the new license key will be displayed automatically. If you want to activate the new features then note the new license key, conclude the activation process, and then use the new license key.

Step 2

The second step of the offline variant is triggered via the Monitor menu “Help” “License data and activation”.

After the offline variant has been selected, select the second step. (Illustration on the left)

A window will open where you can enter the activation code. After you have entered the activation code you can click on the arrow button. (Optionally a new license key can be entered.)

Offline activation is completed with the following window.

The license data is verified and then transferred. Finish the activation dialog when the verification has been concluded.

The software version number may differ from the licensed version number if the license is valid only for an older version.

If you have received a new license key during the offline activation, this key must be entered with step 2 of the offline activation or the activation must be replied.

© NCP engineering GmbH / 1.00